# MONEY LAUNDERING AND TERRORISM: ENFORCEMENT AFTER SEPTEMBER 11TH

ROBERT E. SIMS
MCCUTCHEN, DOYLE, BROWN & ENERSEN, LLP

JANUARY 8, 2002

## I. Global money laundering is now commonly considered a serious national security threat; though nations disagree about definition.

A. Definition in U.S.: Generally, a series of financial transactions used to disguise the illicit source of funds. Funds can be reinvested in further criminal activity or invested in the legitimate economy. Definition includes use of otherwise legitimate funds to promote or facilitate criminal activity, such as terrorism.

B. Drug trafficking (the principal source) and financial crimes (including bank fraud, credit card fraud, and advance fee schemes) are the primary sources of laundered funds worldwide. However, money laundering supports a wide array of other criminal offices, including terrorism, arms trafficking, and alien smuggling.

C. Three stages in most laundering schemes:

1. Placement – Funds, usually currency, introduced to a financial institution. Generally, this is the most vulnerable stage for the money launderer, since large currency transactions are more visible and funds are more closely connected to the underlying criminal offense. Substantial amount of law enforcement and regulatory resources concentrated at this stage.

2. Layering – Usually a series of transactions using multiple financial institutions intended to hide the true source of funds. The use of offshore financial centers, front companies and nominee accounts greatly facilitates the layering process. Transactions become more difficult to detect.

3. Integration – Successfully laundered funds can be invested in the legitimate economy or reinvested in criminal activity. Most difficult stage to detect money laundering.

D. Global money laundering, roughly estimated at $590 billion to $1.5 trillion annually, poses significant national security and foreign policy risks:

1. It is the lifeblood of organize crime worldwide; organizations could not exist without it.

2. Laundering fuels and facilitates official corruption, concentrates money and power in criminals' hands.

3. It can distort markets and undermine the integrity of financial institutions, especially in developing countries.

4. Laundering activity can destabilize developing economies.

5. It allows criminal organizations access to and sometimes control over the legitimate economy.

E. Financing for terrorism poses special challenges:

1. A recent report by the Financial Action Task Force (FATF), the leading international anti-money laundering organization, identified the principal sources of funding for terrorism:

- Drug trafficking
- Extortion and kidnapping
- Robbery
- Fraud
- Gambling
- Smuggling and trafficking in counterfeit goods
- Direct sponsorship by certain states
- Contributions and donations
- Sale of publications (legal and illegal)
- Funds derived from legitimate business activities.

2. With the exception of the last four sources, the FATF report notes that terrorist organizations rely on same sources of funding that organized crime groups utilize. They also use similar methods to launder funds, including:

- Nominee accounts
- Shell companies
- Numbered bank accounts
- Offshore tax havens
- Wire transfers
- Increasing use of professionals (e.g., lawyers, accountants)

FATF plans to provide additional guidance to financial institutions regarding the methods and means of terrorist financing in February 2002. Check FATF website at www1.oecd.org/fatf.

3. Important distinctions between terrorist groups and organized crime:

- Terrorists generally pursue non-financial goals. Most horrific terrorist acts are not intended to generate revenue and may not involve substantial sums of money or suspicious financial transactions. World Trade Center attacks cost approximately $500,000; only one transaction generated a suspicious activity report.

- Otherwise legitimate sources of funding (e.g., states, charitable organizations, legitimate businesses) are difficult to detect.

- Substantial use of underground banking system in some countries.

- Most relevant financial transactions occur at layering and integration stages where money laundering is most difficult to detect.

- Many U.S. and international anti-money laundering measures focus on placement stage and large cash transactions, less effective against terrorist groups. Funds are extremely difficult to trace.

## II. Enforcement After September 11th

A. Adoption of U.S.A. Patriot Act is instructive.

1. Prior to September 11, 2001, anti-money laundering bills prospects were uncertain. White House appeared ambivalent about new regulations and bill had Key House and Senate opponents.

2. After September 11, 2001, anti-money laundering bill flew through Congress as Title III of the U.S.A. Patriot Act, even though many of its provisions have little to do with terrorism.

3. Enforcement likely to be aggressive, stakes higher. Importance of Treasury's Office of Foreign Asset Control (OFAC) reflects view that money laundering is increasingly viewed as a national security issue. Similarly, law gives CIA access to SARs for the first time, including those involving U.S. citizens' accounts.

4. Scope of liability includes not only money laundering statutes (18 U.S.C. §§ 1956 and 1957) and Bank Secrecy Act, but extends to International Emergency Economic Powers Act and other national security legislation. BSA penalties have been strengthened and, under U.S. Sentencing Guidelines, money laundering violations can result in substantially longer prison sentences and higher fines.

- Recent amendments to the Sentencing Guidelines have reduced the disparity between penalties for money laundering and underlying white collar offenses, a constant source of disputes among federal prosecutors and the defense bar for many years. Amendments won't aid defendant convicted of laundering funds for terrorists, however, as penalties remain substantial.

5. Significant law enforcement resources being devoted to this area. Investigators always have the benefit of hindsight. Important for institutions to be in full compliance with the Act and other anti-money laundering laws.

6. White House and Treasury have been more aggressive in targeting groups for sanctions since September 11th.

   - President Clinton used authority under International Emergency Economic Powers Act (IEEPA) for the first time against Colombian drug traffickers in 1995. Treasury relied on substantial evidence collected in various DOJ and international investigations to identify front companies and individuals to target. Initiative had tremendous impact in Colombia – exposed pervasiveness of trafficker influence in the legitimate economy. The largest drug store chain in Colombia was trafficker owned, for example. Initiative was not expanded to other international criminal organizations, largely because evidence was less extensive.

   - Similarly, Congress adopted the Colombia model in passing the Foreign Narcotics Kingpin Designation Act (FNKDA). Under FNKDA, Treasury designates kingpins and imposes IEEPA-like sanctions. To date a relatively small number of drug traffickers in Mexico, Nigeria, Asia and elsewhere have been targeted, but OFAC has done little to identify front companies and supporters.

   - In contrast, the Bush Administration has steadily expanded the scope of the Executive Orders targeting terrorist organizations since September 11th; including charitable organizations and other controversial targets. This indicates a willingness to rely on intelligence information and less extensive evidence than prior initiatives.

B. Goals of U.S. anti-money laundering measures will continue to be in conflict at times.

1. U.S. laws have various goals:

   - Deter money laundering and raise its cost for the launderers.

- Support financial and criminal investigations through record-keeping and suspicious transaction reporting.

- Provide regulatory oversight and protect the reputation and integrity of financial institutions.

- Facilitate criminal prosecution and the forfeiture of criminal proceeds and assets.

2. These goals often conflict:

   - Suspicious transaction reporting may reveal institutional wrongdoing.

   - Good record-keeping may not be enough if regulator or prosecutor believes transaction should have been reported.

   - Institution may be asked to continue a relationship with a customer under investigation.

3. Terrorist/criminal suspect may be beyond government's reach, but the institution that conducted the financial transaction at issue may not be. Non-compliance and other violations of law more likely to come to government's attention.

C. Significant focus on overseas customers and operations.

1. Increase pressure on foreign institutions to cooperate in U.S. investigations.

2. Increase scrutiny on private banking and correspondent accounts.

3. Broader use of asset freezes and forfeitures targeting individuals and groups overseas.

4. U.S. may now deny entry to persons suspected on money laundering offenses overseas.

## III. Protecting the Company: A Six Step Process for Ensuring an Anti-Money Laundering Program Works

A. Appoint a Team

1. Companies appoint a specific team to stay updated on any changes in anti-money laundering legislation and policies, and money laundering trends and techniques. New changes are analyzed with an eye for how they might impact their particular business. Company procedures are then updated to reflect such changes.

2. Remember USA Patriot Act applies more broadly than terrorist financing and is not limited to financial institutions. It will require a reassessment of existing compliance programs, even among institutions with a great deal of experience in this area.

3. Financial institutions should take advantage of the information sharing provisions of the USA Patriot Act, as well as seek more information from the USG.

B. Develop a Targeted Compliance Program

1. A number of non-banking institutions have adopted anti-money laundering programs. For example: Lockheed Martin, Boeing, IBM, General Motors (GM), General Electric (GE), Exxon, the United States Post Office, Proctor & Gamble and Texaco.

2. GE's Anti-Money Laundering Policy includes provisions:

- Requiring each of its businesses to implement "Know Your Customer" procedures and take reasonable steps to ensure that each business does not accept forms of payment identified as means of laundering money.

- Requiring all employees to comply fully with all anti-money laundering laws and regulations.

- Warning employees to watch for particularly suspicious activity, e.g., customer provides insufficient or false information, avoids record-keeping requirements, or makes payments with monetary instruments inconsistent with his or her business activities.

- Warning employees that violation of policies means disciplinary action, including termination. Also warns employees of potential criminal liability.

3. To obtain benefits under the U.S. Sentencing Guidelines and most prosecutors' offices, compliance program cannot simply be a piece of paper; must be able to establish that it targets likely areas of vulnerability for the company and is enforced. Benefits of a strong compliance program can be substantial.

C. Regularly Assess the Risks.

1. Companies should periodically assess how changes in their particular business' risks and characteristics affect vulnerability to money laundering. Policies should then be updated accordingly.

2. Many companies will not launch any new lines of business or sales mechanisms without a money laundering assessment. This is especially important when moving into business relationships outside the U.S.

3. FATF's annual Typologies Report and the U.S. State Department's International Narcotics Control Strategy Report provide useful assessments of current money laundering trends and risks in various regions. The INCSR provides a country-by-country assessment of money laundering issues. FATF also now publicizes an annual list of countries it finds to be uncooperative in the fight against money laundering.

4. Stay informed about OFAC's list of targeted individuals and entities. They are regularly published in the Federal Register and elsewhere. Software programs are available to help screen transactions.

D. Regularly Re-train Employees

1. Businesses should periodically re-train all employees potentially exposed to money laundering.

2. They should also assess the quality of their training programs, including its scope and frequency.

3. Encourage employees to report suspicious activity or internal wrongdoing. Failure to provide an internal reporting mechanism will often lead a concerned employee to report matter to the government.

E. Conduct Annual Audits

1. Companies should conduct annual audits of each department's compliance with the company's anti-money laundering policy.

   a. Include a review of account opening procedures, whether customer names are verifiable, whether high risk accounts are monitored with appropriate frequency, and a review of submitted suspicious activity reports.

   b. Should use internal auditors or outside counsel/auditors for such reviews.

2. Companies should include in an employee's annual review a discussion of his or her adherence to the anti-money laundering policy.

F. Investigate Any Evidence of Internal Wrongdoing and Enforce Policy

1. Don't ignore problems, if they surface.

2. Critically important to conduct internal investigation. Consult counsel and/or internal audit to structure the investigation. Currently a great deal of controversy exists regarding the privileged nature of internal investigations and DOJ requiring waivers of privilege. It is nonetheless generally advisable to maintain the privileged nature of an investigation and defer any assessment of a voluntary waiver.

3. Take disciplinary action when necessary, including consideration of reporting violations and cooperating with law enforcement authorities.